Oresund EFC
iSCSI to FC Gateway
Quickstart Guide
Eli-v6.5.391

Bridgeworks
Unit 1, Aero Centre, Ampress Lane,
Ampress Park, Lymington,
Hampshire SO41 8QF
Tel: +44 (0) 1590 615 444
Email: support@4bridgeworks.com

1 Introduction

This guide is designed to help you through the steps required to power up and configure the basic settings on a Bridgeworks Oresund EFC iSCSI to FC Gateway. For more detailed configuration options please refer to the Oresund EFC iSCSI to FC Gateway Software Manual (https://support.4bridgeworks.com/documents/manuals/).

1.1 Overview

The Oresund EFC iSCSI to FC Gateway creates an interface between a network, which utilises the iSCSI protocol, and devices that reside upon the Fibre Channel Storage Area Network (SAN). The Gateway acts as a two-way interface converting the data packets that are received on the iSCSI network to Fibre Channel data packets. This data is then ready to be sent across a network to Fibre Channel-enabled storage devices such as disks and tape drives.

1.2 Definitions

Throughout this manual, selected terms will be used to describe pieces of equipment and concepts. This section provides an explanation of those terms.

1.2.1 iSCSI Target Device

iSCSI target devices are devices such as disk drives, tape drives or RAID controllers that are attached to the network. Each device is identified by an IQN (iSCSI Qualified Name).

1.2.2 iSCSI Qualified Name (IQN)

Anything connected to a network, be it a computer, printer or iSCSI device must have a unique identifier, such as an IP address, to enable other devices to communicate with it. With iSCSI devices (both targets and initiators) an extra level of identification in addition to the IP address is employed. This is called the IQN. The IQN includes the iSCSI Target's name and an identifier for the shared iSCSI device.
Example: 2002-12.com.4bridgeworks.sdt600a014d10:5

1.2.3 iSCSI Challenge Handshake Authentication Protocol (CHAP)

CHAP is an authentication scheme used by iSCSI to validate the identity of iSCSI targets and initiators. When CHAP is enabled, the initiator must send the correct username and target password to gain access to the iSCSI target.

Optionally the initiator can request that the target authenticates itself to the initiator; this is called mutual CHAP. If mutual CHAP is selected on the initiator, the iSCSI target will authenticate itself with the initiator using the initiator secret.

2 Pre-Install Checklist

Before connecting any equipment, or performing any patching, please ensure you have completed the pre-installation checklist below.

- iSCSI and FC connection details
- iSCSI and FC cables
- IP Addresses for Management interface/s
- PC or Laptop connected to the Management LAN
- Licence Key saved to local machine
- Keyboard and monitor

3 Setup

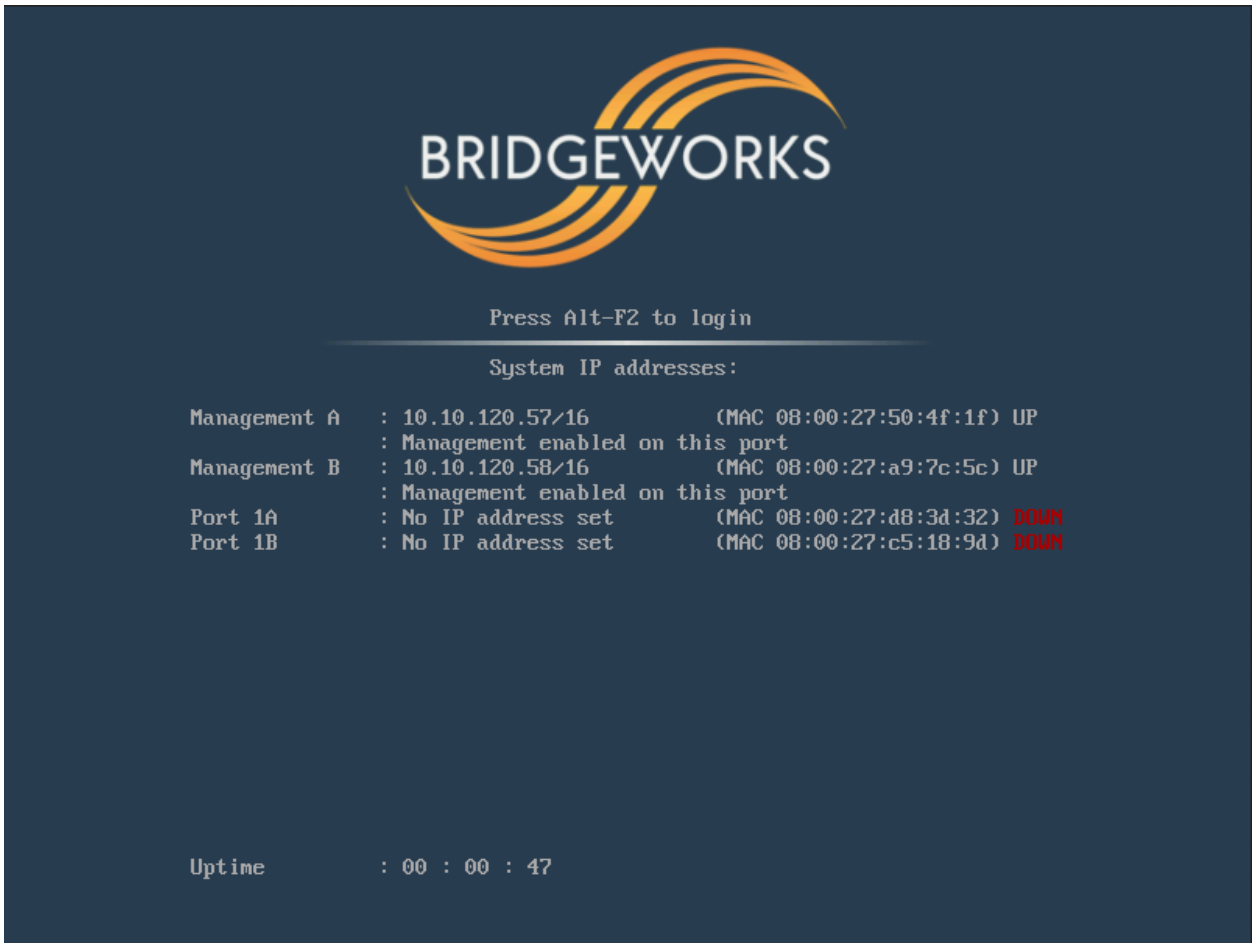
3.1 Hardware

To set up a hardware Oresund EFC iSCSI to FC Gateway:

- Install the server into a rack using the included rails and ensure it is secure.
- Plug the power leads into the appropriate sockets.
- Connect an Ethernet cable to the management interface on Port A of the onboard Network Interface Controller (NIC).
- Connect the iSCSI and FC cables to the appropriate interfaces.
- Connect the keyboard and monitor.

Warning: Ensure that the cables you are using are rated for the correct speed. If a cable is rated for a lower speed than the interface, the connection will not run at full capacity.

Now power on the device. The Gateway should boot with a display similar to the one below:



3.1.1 Configuring a Static IP

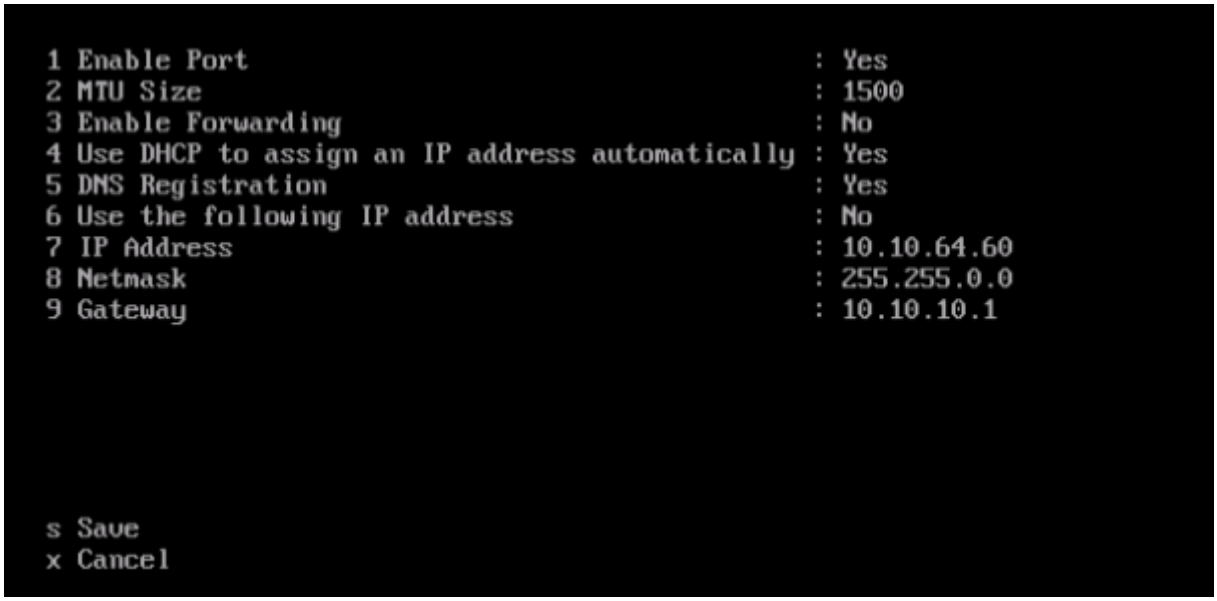
If the device is installed on a network that is not using DHCP you will need to configure a static IP Address so that you can access the Web GUI to complete the configuration of the Gateway.

Press *ALT-F2* to login to the Gateway.

As this will be the first time you have logged into the Gateway you will be required to set an administrator password for the device.

You can now log into the Gateway using the default username *admin*, and the password you set.

Within the Command Line Interface, you can select an option by entering the number next to it. Navigate to Network Connections using 1, then select the port you will be using to manage your Gateway.



Ensure this port is enabled by checking the *Enable Port* option. If this says *No* next to it, select it, then press `y` to enable it.

DHCP will be enabled by default. To set a static IP address for your Gateway, select *Use the following IP address*.

Next, set your IP address by selecting *IP Address* and entering a valid IPv4 address. You may also need to adjust the netmask and default gateway. When you are done modifying your port settings, press `s` to save.

Once you have saved all your settings, press `r` to reboot your Gateway to apply them.

4 Configuration

You can now perform the rest of the configuration remotely via the web interface using the Management IP address.

If you have not used the CLI as above to configure an Admin password, you will be required to set the admin password for the device. This can be altered later on if required. Once set you will be returned to the login screen to enter the username ”admin” with the password you have just configured.

Upon accessing the web interface for the first time, you will be required to accept the End User Licence Agreement.

You should now be on the Home page of the web interface for the Oresund EFC iSCSI to FC Gateway (as shown below).

A guide to configuring the following settings is shown below:

- Section 4.1: Changing the Hostname (Optional)
- Section 4.2: Installing the Licence Key
- Section 4.3: Diagnostics

During the configuration process you will be required to reboot the device several times.

4.1 Changing the Hostname (Optional)

To set the hostname for the device, first return to the Home page using the *Home* button in the sidebar on the left. Then select *Network Connections* and then *General Settings*. You can change

the hostname for the device here. If you wish to display the hostname of the node on the login page select the checkbox labelled ”Hostname on Login Page:”

Once you’ve amended the settings, click *Save* and select *OK* to the prompt that appears. You can make additional configuration changes before rebooting the device.

Return to the Home screen by selecting *Home* at the top left.

4.2 Installing the Licence Key

The licence key for your device contains the licences for the protocols you can connect to.

	Important: If the licence key is not uploaded you will not be able to add the Port Mappings to the ports later on!

To upload the licence key, first navigate to the Home page using the *Home* button in the sidebar on the left. Next select *Licence Key Management*, then *Browse* and locate the licence key file saved to your local machine.

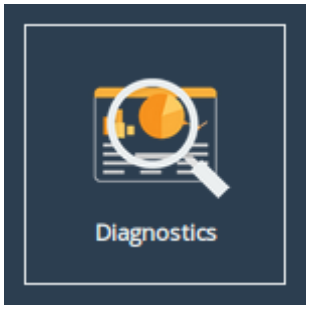
Select the licence key file and then click *Upload*. You should now see which protocols are licensed for your device in the window.

The device requires a reboot for the licence key to take effect. Select *Reboot* from the menu on the left and restart the device.

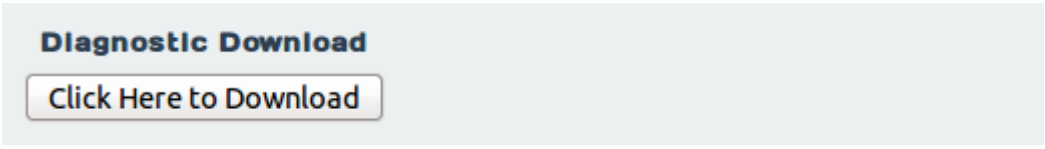
4.3 Diagnostics

In the unlikely event that a problem arises with your Gateway, you may be requested by Bridgeworks Support to provide a diagnostic file.

To download the diagnostic file, click on the *Diagnostics* icon on the Home screen:



Then click on the *Click Here to Download* button.



This will cause the Gateway to collect data regarding various modules and store them in a single

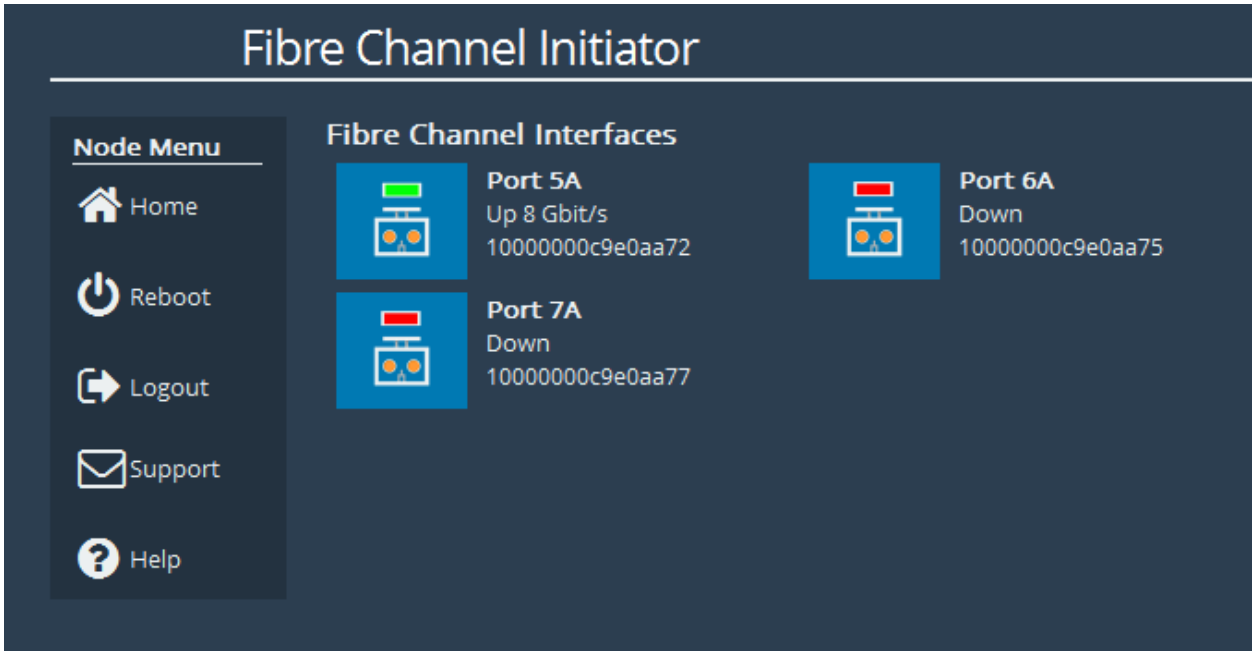
file. Once this process is complete, a download for “diagnostics.bin” will begin.

5 Fibre Channel Initiator Connections

This configuration page allows the administrator to configure ports designated as Fibre Channel Initiator interfaces.

From the Home screen of the web interface, select the *FC Initiator* icon from the *Devices and Protocols* section.

You will see the following page:



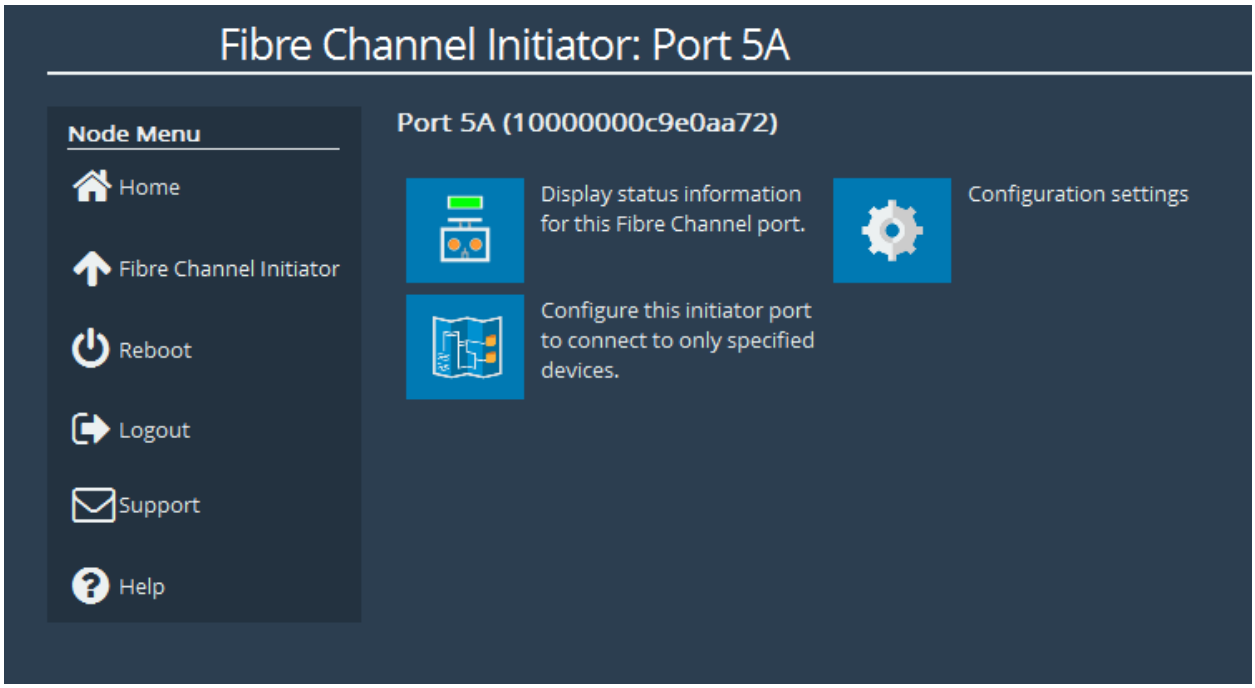
This page lists each Fibre Channel port which has been designated as an initiator. Three pieces of information are displayed about each port next to an icon. In order they are:

Port designation the number is the designation of the PCI slot, and the letter ‘A’ or ‘B’ denotes that this is the left, or right-hand port of that slot, respectively.

Current state This shows whether the Fibre Channel link for this port is up or down, and the speed of the link if it is currently up.

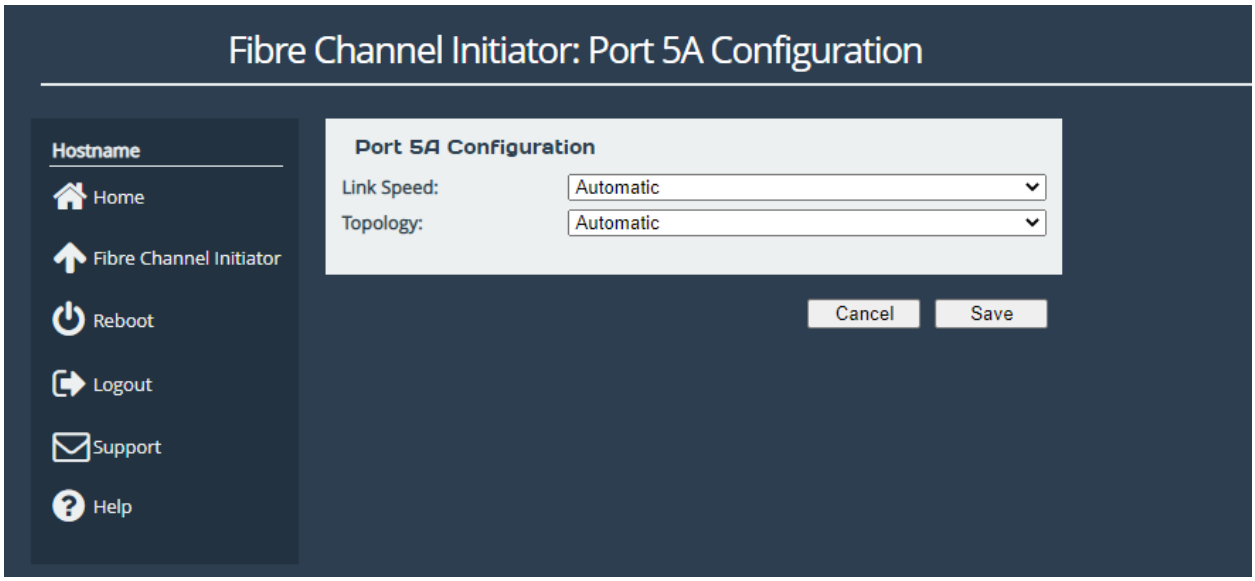
WWPN The unique World Wide Name identifier for this port.

Selecting one of the icons will navigate to the page for that initiator port, with 3 options:



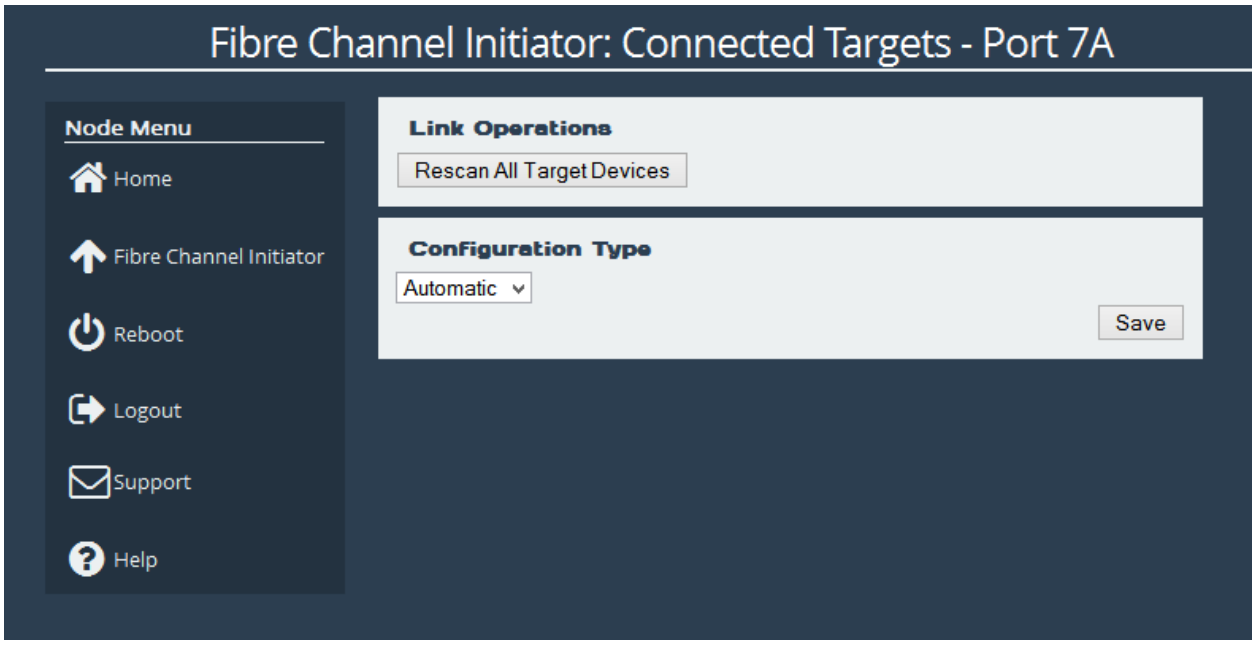
Display status information for this Fibre Channel port allows you to see verbose information about the Fibre Channel port.

Configuration settings allows you to manually configure the *Link Speed* and *Port Topology*:

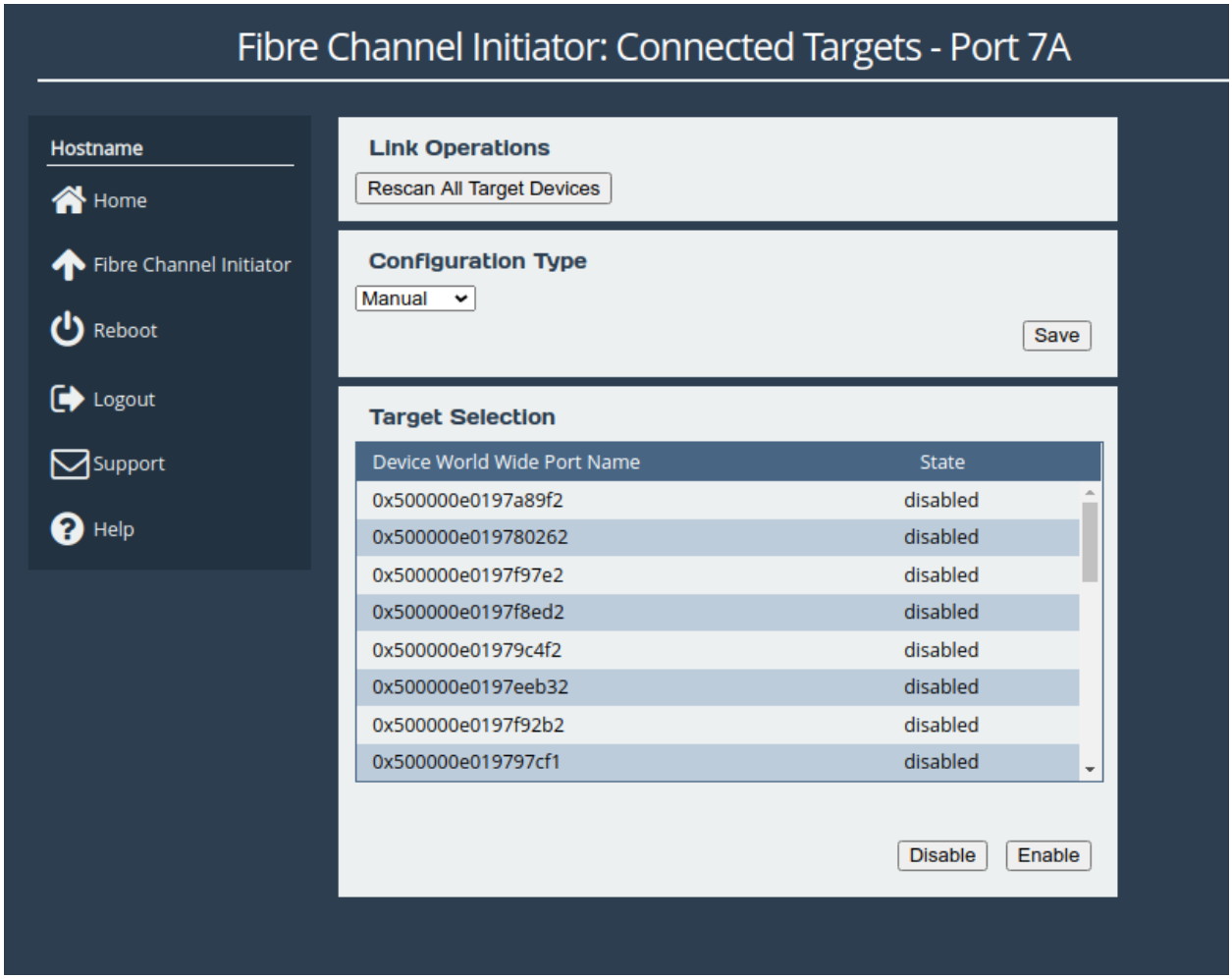


1. The *Link Speed* can be set to *Automatic* or one of the speeds supported by the Fibre Channel port. In most cases this option may be left set to *Automatic*. If you are unsure, set the link speed to the SFP speed. This option is not available on some products.
2. The *Topology* pull down menu has 3 options: *Automatic*, *Loop (arbitrated Loop, FC-AL)*, and *Point-to-Point (FC-P2P)*. It is recommended that you leave this option at *Automatic* unless you wish to force the link into a known topology.

Configure this initiator port to connect to only specified devices allows you to disable certain connected Fibre Channel targets.



The default configuration type is set to *Automatic*. Using the *Configuration Type* drop down, you can change this to manual. This allows you to enable or disable each individual target on the Fibre Channel link.



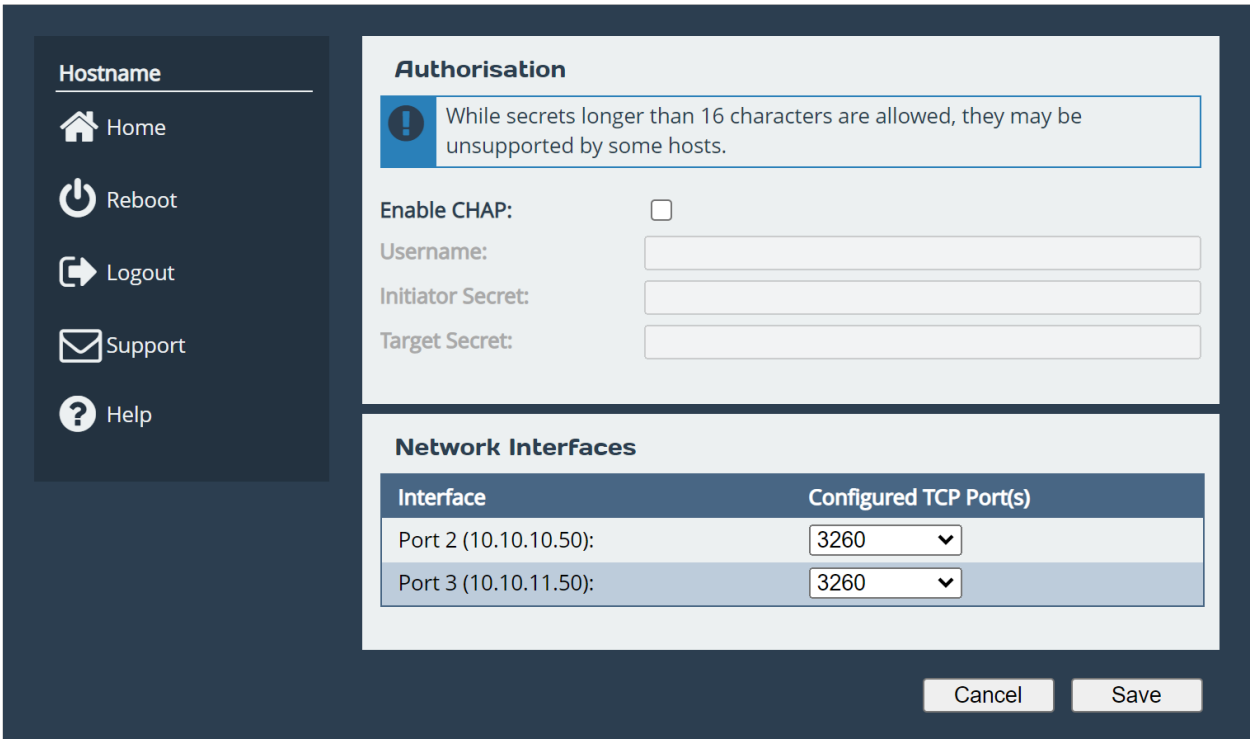
Select the FC target by clicking on its World Wide Port name, and then click *Enable* or *Disable*.

6 iSCSI Target Configuration

This page allows you to configure mutual CHAP authorisation, and TCP ports of each iSCSI target interface.

From the Home screen of the web interface, select the *iSCSI Target* icon under the *Devices and Protocols* section.

The web interface will then display the following:



6.1 Authorisation (CHAP)

CHAP is an authentication scheme used by servers to validate the identity of clients, and vice versa. When CHAP is enabled, the initiator must send the correct username and target password to gain access to the iSCSI target of the Gateway.

The initiator secret is provided to allow iSCSI mutual CHAP. If mutual CHAP is selected on the initiator, the iSCSI Bridge will authenticate itself with the initiator using the initiator secret.

To enable CHAP, select the *Enable CHAP* checkbox and enter the following details:

Username This is the same name as specified on the initiating host.

Initiator Secret This is the password defined on the initiating host. This must be 12 to 256 characters long. This should only be entered if mutual CHAP is enabled on the initiating host.

Target Secret This is the password that must be entered on the initiating host. This must be 12 to 256 characters long.

6.2 Network Interfaces

The table under the Network Interfaces section displays the interfaces and IP addresses the iSCSI target is presenting devices on.

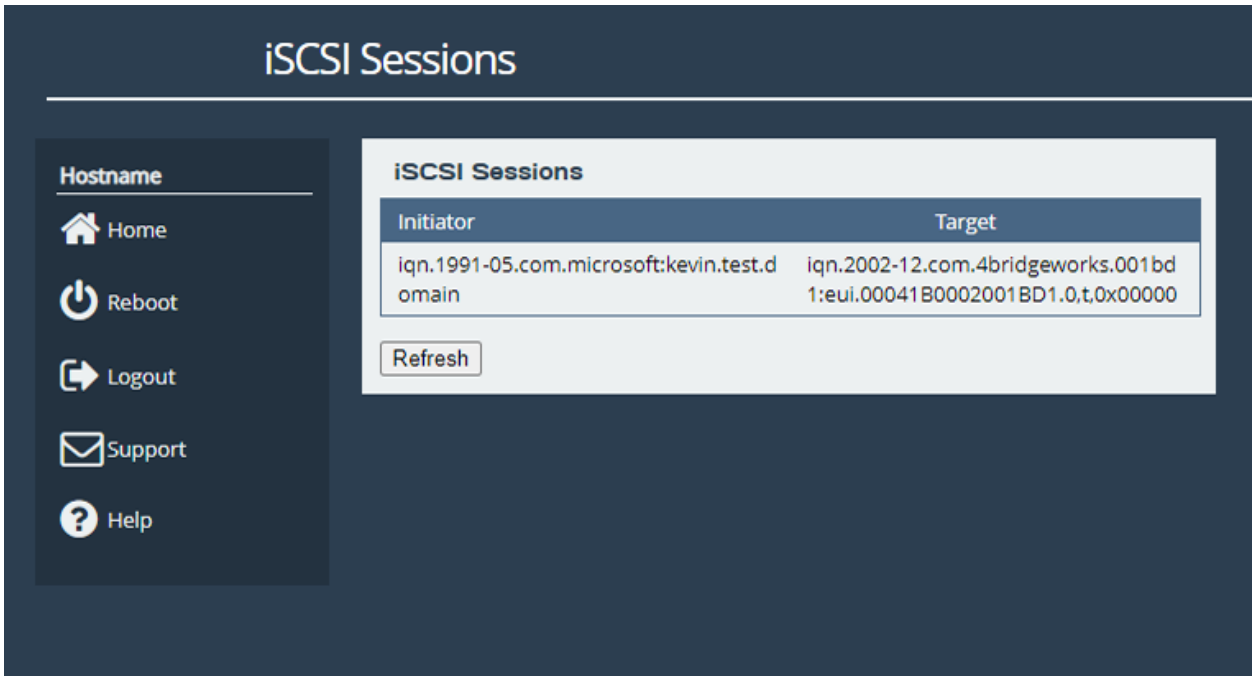
The iSCSI protocol officially uses two main TCP ports: 3260 and 860. For each iSCSI target interface, you can choose to enable either one these TCP ports, or both, or disable iSCSI on the interface completely, from the *Configured TCP Port(s)* dropdown.

6.3 iSCSI Sessions

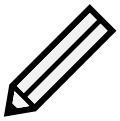
Each initiator will open at least one session with each target device it is logged on to. The iSCSI Sessions page in the web interface of the Gateway can be used to review these connections.

From the Home screen, select the *iSCSI Sessions* icon under the *Devices and Protocols* section.

The web interface will then display the following:



This page lists current connections to iSCSI initiators. The IQN of the initiator is shown in the *Initiator* column, and the IQN of the device it is logged on to is shown in the *Target* column. See Section 1.2.2: iSCSI Qualified Name (IQN) for more information.

	Note: It is possible that more than one initiating host may be connected to any target device, one host to multiple target devices, or one host has multiple connections to a single device.

7 Additional Features

Congratulations on finishing the basic setup of your Oresund EFC iSCSI to FC Gateway. Consider browsing the manuals for a complete list of capabilities (available at https://support.4bridgeworks.com/documents/manuals/).

The following sections are recommended starting points for some useful additional features.

7.1 iSNS

iSNS enables automatic discovery of iSCSI devices by your Oresund EFC iSCSI to FC Gateway.

To enable iSNS, see the Internet Storage Name Service (iSNS) section of the Oresund EFC iSCSI to FC Gateway Software Manual.

8 Useful Links

Further documentation and support is available through our website: https://support.4bridgeworks.com/

If your question is not answered in our documentation, please submit a ticket: https://support.4bridgeworks.com/contact/